IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Craig H. Rowland
Application No.:	10/685,726
Filed:	October 15, 2003
Confirmation No.:	5392
Art Unit:	2131
Examiner:	Aravind K. Moorthy
Title:	METHOD AND SYSTEM FOR REDUCING THE FALSE ALARM RATE OF NETWORK INTRUSION DETECTION SYSTEMS

Mail Stop - AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicant respectfully requests reconsideration of the Application in light of the remarks set forth below.

REMARKS

Applicant contends that the rejections of Claims 1-21 contain clear legal and factual deficiencies, as described below. Applicant requests a finding that these rejections are improper and that the claims are allowable.

Section 102 Rejections

The Final Office Action mailed May 30, 2007 ("Final Office Action") and the Advisory Action mailed August 15, 2007 ("Advisory Action") reject Claims 1-21 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,152,105 to McClure et al. ("*McClure*"). Applicant requests a finding that these rejections are improper and that the claims are allowable.

Applicant respectfully submits that *McClure* fails to disclose, teach, or suggest elements specifically recited in Applicant's claims. For example, *McClure* fails to disclose, teach, or suggest the following recited in independent Claim 1:

> receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host.

The Examiner relies on the passages at Col. 24, Lines 11-21 ("Passage A") and Col. 17, Line 29 - Col. 18, Line 50 ("Passage B") of *McClure* to teach these elements. (Final Office Action, Page 2 (quoting the passage of *McClure*), Page 3; *see also* Advisory Action, Continuation Sheet (quoting the passage of *McClure*).) According to Passage A:

> Sometimes, in order to "force" a response from the target computer, ***an intruder*** may send a ***malformed packet*** to a target port. While this known technique increases the likelihood that an open UDP port on the target computer can be identified, this technique also substantially increases the likelihood that the malformed packet could ***damage the target computer***. Also, firewalls or routers may detect and filter out malformed packets, and such packets can alert the target network of an attempted security breach.
>
> ***The intelligent UDP port scanning test in accordance with this embodiment of the present invention employs an efficient, less intrusive and more accurate method for scanning UDP ports on a target computer.***

(*McClure*, Col. 24, Lines 11-26 (emphasis added).)

Passage B merely discloses packets used to identify an operating system. (*McClure*, Col. 17, Line 36 - Col. 18, Line 3; *see also McClure*, Col. 18, Lines 43-44 (stating "[b]elow

is an example exchange of packets when performing an OS [operating system] identification").)

Passages A and B fail to disclose, teach, or suggest the above recited element. First, as explained in Passage A, a malformed packet is sent by ***an intruder***. ***An intruder*** sending a malformed packet, as is relied upon by the Examiner, fails to disclose "receiving, ***from a network intrusion detection sensor***, one or more data packets associated with an alarm indicative of a potential attack on a target host" of Claim 1 (emphasis added).

Second, the packets of Passage A are completely different from the packets of Passage B, and thus cannot disclose, teach, or suggest the packets of Claim 1. Passage A clearly discloses that a technique of forcing a response using a malformed packet is not used in the system of *McClure* because the technique could damage a computer. That is, the malformed packets of Passage A are not used in the system described by Passage B.

Furthermore, *McClure* clearly discloses that the packets of Passage B are RFC-compliant TCP packets. (*McClure*, Col. 14, Lines 41-56; *see also McClure*, Col. 16, Line 57 - Col. 17, Line 4.) The RFC-compliant TCP packets of Passage B, however, are not the malformed packets of Passage A:

> The use of RFC-compliant TCP packets advantageously ***reduces the probability that the detection packets are blocked by a router or firewall, and greatly reduces the probability that the detection packets will cause damage or crashes at the target computer***.

(*McClure*, Col. 16, Lines 62-67 (emphasis added).) That is, the packets of Passage B greatly reduce the problems associated with the malformed packets of Passage A. As a result, *McClure* fails to disclose "receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host" of Claim 1.

Consequently, at a minimum, *McClure* fails to disclose, teach, or suggest the elements of independent Claim 1. For at least these reasons, Applicant contends that the rejection of Claim 1 is improper, as are the rejections of its dependent claims. For the same or analogous reasons, the rejections of Claims 7 and 16 are improper, as are the rejections of their dependent claims. Accordingly, Applicant requests a finding that these rejections are improper and that Claims 1-21 are allowable.

CONCLUSION

As the rejections of Claims 1-21 contain clear deficiencies, Applicant respectfully requests a finding that Claims 1-21 are allowable. To the extent necessary, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Keiko Ichiye
Reg. No. 45,460

KI/BD

Correspondence Address:

Customer Number: 05073

Date: August 30, 2007